

ECS Configuration Change Request

Page 1 of 1 Page(s)

1. Originator Byron V. Peters	2. Log Date: 3/5/03	3. CCR #: 03-0150	4. Rev: —	5. Tel: 301/883-4077	6. Rm #: 2013	7. Dept. SE
8. CCR Title: Test sendmail fixes						
9. Originator Signature/Date Byron V. Peters /s/ 3/5/03			10. Class IN	11. Type: CCR	12. Need Date: 3/6/03	
13. Office Manager Signature/Date James R. Mather /s/ 3/5/03			14. Category of Change: Initial ECS Baseline Doc.		15. Priority: (If "Emergency" fill in Block 27). Emergency	
16. Documentation/Drawings Impacted (Review and submit checklist): will be included in next releases			17. Schedule Impact:		18. CI(s) Affected: CSS, ISS	
19. Release Affected by this Change: 6A		20. Date due to Customer:		21. Estimated Cost: None - Under 100K		
22. Source Reference: <input checked="" type="checkbox"/> NCR (attach) <input type="checkbox"/> Action Item <input type="checkbox"/> Tech Ref. <input type="checkbox"/> GSFC <input type="checkbox"/> Other: ECSed36965						
23. Problem: (use additional Sheets if necessary) CERT has published an alert on vulnerabilities found in sendmail that affects ECS services.						
24. Proposed Solution: (use additional sheets if necessary) Test an IBM-provided fix on the VATC Portus firewall and upgrade the t1ins01 with the Sun 110615-05 patch						
25. Alternate Solution: (use additional sheets if necessary) N/A						
26. Consequences if Change(s) are not approved: (use additional sheets if necessary) The patches may not function correctly in the field causing downtime.						
27. Justification for Emergency (If Block 15 is "Emergency"): There is significant concern at the DAACs at the exposure risk that this vulnerability poses and immediate relief is required.						
28. Site(s) Affected: <input type="checkbox"/> EDF <input type="checkbox"/> PVC <input checked="" type="checkbox"/> VATC <input type="checkbox"/> EDC <input type="checkbox"/> GSFC <input type="checkbox"/> LaRC <input type="checkbox"/> NSIDC <input type="checkbox"/> SMC <input type="checkbox"/> AK <input type="checkbox"/> JPL <input type="checkbox"/> EOC <input type="checkbox"/> IDG Test Cell <input type="checkbox"/> Other						
29. Board Comments:			30. Work Assigned To:		31. CCR Closed Date:	
32. EDF/SCDV CCB Chair (Sign/Date): A. Abtahi /s/ 03/06/03			Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS			
33. M&O CCB Chair (Sign/Date):			Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS			
34. ECS CCB Chair (Sign/Date):			Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ESDIS			

ADDITIONAL SHEET

CCR #: 03-0150 **Rev:** — **Originator:** Byron V. Peters

Telephone: 301/883-4077 **Office:** SE

Title of Change: Test sendmail fixes

For the Firewall accomplish the following procedure:

Setting up the install:

1. Login to the firewall.

2. You can download all files from AIX directly from the firewall. Use anonymous as user and your email address for the password. You need the 'bos.net.tcp.client.4.3.3.87' filesets loaded in order to "ensures that the proper versions of co-requisite system files, such as libc.a, are installed". All sites have done Maintenance Release 10 so you will be at bos.net.tcp.client.4.3.3.85'. You can check with the following command:

```
# lspp -L bos.net.tcp.client
```

This will show the following:

Fileset	Level

bos.net.tcp.client	4.3.3.85

3. Before the install and the last number will be 7 after the install. Log in as root and create two directories, one for the bos.net.tcp.client (tcpfix) and one for the sendmail (efix) fix. Type the following commands:

```
#mkdir /tmp/tcpfix  
#mkdir /tmp/efix
```

4. Now ftp to IBM and get the files with the following commands:

```
#ftp techsupport.services.ibm.com  
ftp> get /aix/fixes/v4/os/bos.net.tcp.client.4.3.3.87.bff  
ftp> get /tmp/tcpfix/bos.net.tcp.client.4.3.3.87.bff
```

Notice the ending of 'bff' must have it in order to get the file. Cannot do 'ls' because there are too many files and you will get an error message. Stay log on and also download the sendmail fix at the same time. Type the following commands:

```
ftp> get /aix/efixes/security/sendmail_efix.tar.Z /tmp/efix/sendmail_efix.tar.Z
```

5. You should from another windows make sure you have using the command:

```
# ls /tmp/tcpfix  
/tmp/tcpfix/bos.net.tcp.client.4.3.3.87.bff  
# ls /tmp/efix  
/tmp/efix/sendmail_efix.tar.Z
```

6. You will first install bos.net.tcp.client file set. Load bos.net.tcp.client File Set —. Change directory to /tmp/tcpfix.

```
#cd /tmp/fixes
```

7. Then type the following command:

```
#inutoc .
```

8. This will build the '.toc' file the installation program needs. Start SMIT.

```
#smit
```

The first menu heading will read:

Software Installation and Maintenance

Click on the box labeled as follows:

Install and Upgrade Software

Click on the box labeled as follows:

Install and Update from LATEST Available Software

A new menu will pop up. It will display the message/question "INPUT device / directory".

Write in the directory path '/tmp/tcpfix' where the files are located. Click on 'OK' button.

Next menu will pop up. Take all the defaults. Click on 'OK' button to continue.

A new dialog box will display 'Are You Sure', click on 'OK' button to start installing the file sets. Estimated installation time is less than 10 minutes.

9. After the files are installed you have must re-boot the firewall with the command:

```
#shutdown -r now
```

Sendmail Binary —

1. After the firewall reboots, login then uncompress and un-tar the sendmail file. You will have to do the following steps. First change to the directory with sendmail_efix.tar.Z file:

```
# cd /tmp/efix
```

2. Uncompress it and un-tar the resulting tar file.

```
# uncompress sendmail_efix.tar.Z
```

```
# tar xvf sendmail_efix.tar
```

```
# cd sendmail_efix
```

3. You will see a set of files. The appropriate for our OS level is 'sendmail.433'. Now rename the patched binary files and set ownership and permissions.

```
# mv sendmail.433 sendmail
```

```
# chown root.system sendmail
```

```
# chmod 6551 sendmail
```

4. Create a backup copy of original binary. Remove all permissions from the backup copy.

```
# cd /usr/sbin
```

```
# cp sendmail sendmail.orig
```

```
# chmod 0 sendmail.orig
```

5. Replace the current system binary with the patched binary. Use the -p option to preserve the file permissions set in step 3.

```
# cp -p /tmp/efix/sendmail_efix/sendmail /usr/sbin/sendmail
```

6. Logoff

For the Solaris sendmail system:

1. Login as root or su to root.

2. Download the 110615-05 patch from Sun to /var/spool/pkg

3. Verify the md5 signature

3. Add the patch using the command:

```
# pkgadd 110615-05
```

Answer "y" to all questions. Verify that the patch was successfully installed from the verbage at the end of the install.

4. Logoff